IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Appellants:	Mendonca et al.	Patent Application	
Application No.:	10/627,017	Group Art Unit:	2436
Filed:	July 25, 2003	Examiner:	Okoronkwo, C.

For: METHOD OF MANAGING UTILIZATION OF NETWORK INTRUSION DETECTION SYSTEMS IN A DYNAMIC DATA CENTER

REPLY BRIEF

In response to the Examiner's Answer mailed on February 13, 2009, Appellants respectfully submit the following remarks.

REMARKS

Appellants are submitting the following remarks in response to the Examiner's Answer mailed on February 13, 2009 (hereinafter, "Examiner's Answer). In these remarks, Appellants are addressing certain arguments presented in the Examiner's Answer. While only certain arguments are addressed in this Reply Brief, this should not be construed that Appellants agree with the other arguments presented in the Examiner's Answer.

Response to Argument on Page 8, Section A, First Paragraph, through Page 10, First Paragraph, of the Examiner's Answer

In the Appeal Brief filed November 17, 2008, while addressing a 35 U.S.C. §102(e) rejection of Claims 1-20, and in particular independent Claim 1, Appellants argue that Shanklin (U.S. Patent Application No. 6,578,147) (hereinafter, "Shanklin") does not anticipate:

> providing a plurality of network intrusion detection systems, each being networked so that utilization of each network intrusion detection system can be based on demand for said network intrusion detection systems in said dynamic data center;
> receiving a monitoring policy and a plurality of monitoring points to be monitored on a network with any of said network intrusion detection systems; and
> automatically arranging the monitoring of said monitoring points using said network intrusion detection systems and said monitoring policy.

(Emphasis in original; Appeal Brief filed on November 17, 2008, page 8, third paragraph.)

Furthermore, Appellants pointed out that the Office Action mailed on August 5, 2008 (hereinafter, "August 5, 2008 Office Action") states:

> [r]egarding the second limitation ["receiving a monitoring policy…], the Examiner directs the Applicant to column 2 lines 1-13 in which Shanklin et al. discloses the

claimed "monitoring policy" as being inclusive to the IDS sensors, which comprise: "packet load to the sensors that is 'load balanced', such that said packets are distributed at least at a session-based level [or] packet-based level … the results of the detection performed by the sensors and the network analyzer are used to determine if there is an attempt to gain unauthorized access to the network.

(Emphasis in original; August 5, 2008 Office Action.)

In response to the August 5, 2008 Office Action's foregoing statement, Appellants argued the following in the Appeal Brief filed on November 17, 2008:

The instant Office Action seems to be equating Shanklin's session-based and packet-based load balancing with "receiving a monitoring policy and a plurality of monitoring points to be monitored on a network with any of said network intrusion detection systems" as is recited in Appellants' Claim 1.

Shanklin further describes "session-based" and "packet-based" load balancing. For example, Shanklin describes session-based load balancing as the following:

> that each sensor 21 handles a portion of the sessions incoming to the network. A stream of packets, S1, S2, … S6, … is illustrated. In the example of FIG. 2, the load balancing is such that S1 goes to a first sensor, S2 to a second, S3 to a third, S4 to the first, and so on. Thus, each sensor 21 handles one-third of the sessions in a given datastream.

(Emphasis added; Shanklin, Column 5, lines 21-29.) Shanklin describes packet-based load balancing to mean the following:

> Router 32 has a load balancing unit 32a, which distributes a packet stream comprised of packets P1, P2, … P6 …. The load balancing is such that P1 goes to a first sensor, P2 to a second, P3 to a third, P4 to the first, and so on.

(Shanklin, column 5, lines 56-62.)

Appellants understand Shanklin to disclose a session-based load balancing in which a session of a series of sessions are distributed to each sensor of multiple sensors, and a packet-based load balancing in which packets are distributed to each sensor of multiple sensors. Shanklin focuses on distributing sessions and packets to and among all sensors that detect "signatures of attacks" (Shanklin, column 5, line 37). However,

> Shanklin remains silent as to a dynamic system that receives "a monitoring policy and a plurality of monitoring points to be monitored" (emphasis added) as is recited in Appellants' Claim 1.

(Emphasis in original; Appeal Brief filed on November 17, 2008.)

In the response to this argument, the Examiner's Answer asserts that "…nowhere in the claim language is there mention of a dynamic system. Instead the claim language contains the limitations mentioning of only a dynamic data center…" (Examiner's Answer, page 8, section A, first paragraph). The Examiner's Answer also states:

> [t]he Examiner is clarifying that the monitoring or "security policy" disclosed by Shanklin, that is provided by the administrator and is configured into each monitoring device or sensor (thus making it inclusive to the sensor) is what is being equated to the claimed and argued, "receiving a monitoring policy and a plurality of monitoring points to be monitored on a network with any of said network intrusion detection system."

(Emphasis added; Examiner's Answer, page 10, section A, first paragraph.)

Appellants respectfully submit and reiterate that Shanklin remains silent as to a dynamic data center (Appellants' Claim 1) or a system comprising a dynamic data center (Appellants' Claim 15) that receives "a monitoring policy and a plurality of monitoring points to be monitored" (emphasis added) as is recited in Appellants' Claim 1 and 15. Instead, Appellants understand Shanklin to focus on a session-based load balancing in which a session of a series of sessions are distributed to each sensor of multiple sensors, and a packet-based load balancing in which packets are distributed to each sensor of multiple sensors. In total, Shanklin focuses on distributing sessions and packets to and among all sensors that detect "signatures of attacks"

(Shanklin, column 5, line 37), not a dynamic data center that receives "a monitoring policy **and** a plurality of monitoring points to be monitored" as is recited in Appellants' Claim 1.

Therefore, Appellants respectfully submit that Shanklin does not anticipate the features as are set forth in Appellants' independent Claim 1, and as such, Claim 1 traverses the Examiner's basis for rejection under 35 U.S.C. §102(e) and is in condition for allowance. Accordingly, Appellants also respectfully submit for similar reasons that Shanklin does not anticipate the features as are recited in Claims 8 and 15. Furthermore, Appellants respectfully submit that Claims 2-7 depending on Claim 1, Claims 9-14 depending on Claim 8, and Claims 16-20 depending on Claim 15 overcome the rejection under 35 U.S.C. §102(e) as being dependent on an allowable base claim.

CONCLUSION

In view of the above remarks, Appellants continue to assert that Shanklin does not anticipate the features of Appellants' Claims 1-20 for the reasons presented above and for the reasons previously presented in the Appeal Brief filed on November 17, 2008.

Respectfully submitted,

WAGNER BLECHER LLP

Dated: 04/07/2009

/John P. Wagner, Jr./
John P. Wagner, Jr.
Registration Number: 35,398

WAGNER BLECHER
123 Westridge Drive
Watsonville, CA 95076
(408) 377-0500